CLAIMS

1. A method of processing a digital audio signal comprising the steps of:

a) providing a digital audio signal representing unimpaired audio information;

b) compressing and encrypting the said digital audio signal to produce a first compressed and encrypted audio signal, the audio information of which is substantially unimpaired compared to that of the said digital audio signal;

c) producing an unencrypted second audio signal; and

d) combining the said first and second audio signals to produce a combined signal comprising the said compressed and encrypted first audio signal and the unencrypted second audio signal.

2. A method according to claim 1 wherein the digital audio signal is losslessly compressed to produce the said first audio signal.

3. A method according to claim 1 or 2, wherein the said first audio signal occurs as noise in the said combined signal.

4. A method according to claim 3, wherein the step of combining the first and second signals comprises embedding the first signal as noise in the second signal.

5. A method according to claim 1, 2 or 3, wherein the step of combining comprises appending at least part of the first signal to the said second signal.

6. A method according to claim 1, 2, 3 or 4, wherein the step of producing the said second signal comprises impairing the digital signal.

7. A method according to claim 5, wherein the step of producing the said second signal comprises combining the said digital signal with a third signal which impairs the digital signal.

8. A method according to claim 5, comprising the steps of modulating the said third signal and combining the modulated third signal with the said digital signal.

9. A method according to any preceding claim, wherein the step of producing the first signal comprises compressing the digital signal and encrypting the compressed signal without substantially increasing the number of bits of the compressed digital signal.

10. A method according to any preceding claim wherein the said second signal is a sampled digital signal, each sample having most significant bits (hereinafter MSBs) and less significant bits (hereinafter LSBs).

11. A method according to claim 10, wherein the digital signal is in fixed point format.

12. A method according to claim 10 or 11, wherein the first signal is combined with the said second signal by replacing the LSBs of the said second signal with at least some of the bits of the first signal.

13. A method according to claim 12, wherein a predetermined fixed number of LSBs of the said second signal are replaced by at least some of the bits of the first signal.

14. A method according to claim 12, wherein, in the combined signal, the ratio of MSBs (representing the said second signal) to LSBs (representing the bits of the first signal) is variable.

15. A method according to claim 14, wherein the said ratio is dependent on the amount of compression applied to the first digital signal.

16. A method according to claim 12, 13, 14 or 15, wherein the combined signal includes data indicating which bits of the combined signal are LSBs and which bits are MSBs.

17. A method according to any one of claims 10 to 16, comprising the step of reducing the amount of data in the said second signal.

18. A method according to claim 17, comprising the step of reducing the sampling rate of the said second signal.

19. A method according to any one of claims 10 to 18, comprising providing a file containing the said first signal and a file containing the said second signal.

20. A method according to claim 19, wherein the ratio of MSBs (representing the said second signal) to LSBs (representing said first digital signal) is dependent on the number of bits in the files of the first signal and of the second signal.

21. A method according to claim 19, wherein the bits of the first signal are distributed over samples of the second signal in dependence on the ratio of the total number of encrypted bits in the encrypted signal file to the total number of samples of the said second signal.

22. A method according to claim 21, wherein the said ratio is approximated by an integer fraction M/N, and comprising the steps of selecting groups of N samples and distributing, over the N samples of each group, corresponding sets of M bits.

23. A method according to claim 22, comprising the steps of

a) scaling the value A of each of the N samples according to $A'[X] = (A[X]/S) * S$ where: X is an ordinal numbering of the samples and equals 0 to N-1; and $S = 2^R$ where R is M/N; and

b) replacing $A'[X]$ by $A''[X] = A'[X] + V/S^X$ for $X > 0$, and

by $A''[0] = A'[0] +$ mod S for $X = 0$,

where for each of X= N-1 to 0, V is replaced by $V-V/S^X$, V initially being the value of the M bits when X=N-1.

24. A method according to any one of claims 1 to 11, wherein the said second signal is a sampled digital signal, each sample having most significant bits (hereinafter MSBs) and less significant bits (hereinafter LSBs), and comprising the step of dividing the said second signal into blocks each block comprising a plurality of samples.

25. A method according to claim 24, wherein all the blocks of the said second signal contain the same predetermined number of samples.

26. A method according to claim 24 or 25, comprising the step of analysing the signal level of the said second signal, and setting the number of samples per block in dependence on signal level.

27. A method according to claim 24, wherein the number of samples per block in the said second signal varies.

28. A method according to claim 27, comprising the steps of analysing the signal level of the said second signal, and setting the number of samples in a block in accordance with a function of the levels of the signal samples within the block.

29. A method according to any one of claims 24 to 28, comprising providing, in the said second signal, data indicating the boundaries of the blocks.

30. A method according to claim 29, wherein, in each block, the first signal is combined with the said second signal by replacing the LSBs of the said second signal with bits of the first signal and the ratio of MSBs (representing the said second signal) to LSBs (representing the bits of the first signal) in each block is a function of the signal levels of the samples of the said second signal in the block.

31. A method according to claim 30, wherein the said data indicating the block boundaries includes data indicating the number of samples in each block.

32. A method according to any one of claims 1 to 11, wherein the step of producing the first signal comprises the steps of compressing and then encrypting the said digital audio signal, and wherein at least the step of encrypting comprises selecting sections of the compressed digital audio signal, separately encrypting each section, and further comprising the step of providing data in the first signal indicating the section boundaries.

33. A method according to claim 32, comprising providing a file containing the said digital audio signal to be compressed and encrypted.

34. A method according to claim 33, comprising the steps of compressing the whole file and then encrypting the said sections of the compressed file.

35. A method according to claim 33, comprising the steps of selecting sections of the file, separately compressing and encrypting each section and providing each section with data at least identifying the section.

36. A method according to any one of claims 32 to 35, comprising the steps of encrypting at least one section according to one encryption key, encrypting at least one other section according to another key, and storing data indicating the correspondence between the sections and the keys.

37. A method according to claim 36, wherein the said correspondence data is stored in the first digital signal.

38. A method according to any one of claims 32 to 37, wherein the said data indicating the section boundaries identify the data included in the sections.

39. A method according to any one of claims 1 to 37, comprising the step of compressing at least part of the said second signal and wherein the said combining step comprises combining the first signal with the compressed second signal.

40. A method according to claim 39, when dependent on any one of claims 1 to 16, wherein the said compressed second signal comprises auxiliary data space within the data structure thereof, and comprising the step of placing at least some of the bits of the first digital signal in the said auxiliary data space of the compressed second signal.

41. A method according to claim 39 or 40, wherein the second signal is compressed according to an MPEG standard.

42. A method according to claim 10 or 11, wherein the step of producing the first digital signal comprises receiving the digital signal from a streaming source, dividing the digital stream into segments each comprising a predetermined number of samples, and separately compressing and encrypting each segment.

43. A method according to claim 42, comprising encrypting all sections according to the same key or encrypting at least one section according to one encryption key, and at least one other section is encrypted according to another key and storing data indicating the correspondence between the sections and the keys.

44. A method according to claim 43, wherein the said correspondence data is stored in the first digital signal.

45. A method according to claim 42, 43 or 44, wherein the first signal is combined with the said second signal by replacing, in samples of the second signal, the LSBs of the said second signal with the bits of the first signal.

46. A method according to claim 45, wherein a predetermined fixed number of LSBs of a sample of the said second signal are replaced by the bits of the first signal.

47. A method according to claim 46, wherein, in samples of the combined signal, the ratio of MSBs (representing the said second signal) to LSBs (representing the bits of the first signal) is variable.

48. A method according to claim 47, wherein the said ratio is dependent on the amount of compression applied to the first signal.

49. A method according to claim, 45, 46, 47 or 48, wherein the combined signal includes data indicating which bits of the combined signal are LSBs and which bits are MSBs.

50. A method according to claim, 45, 46, 47, 48 or 49, comprising appending at least part of the first digital signal to the said second signal.

51. A method according to claim 42, 43 or 44, comprising the steps of selecting groups of N samples and distributing over the N samples of each group corresponding sets of M bits of the first signal, where the ratio M/N is an integer fraction.

52. A method according to claim 51, comprising the steps of

a) scaling the value A of each of the N samples according to $A'[X] = (A[X]/S) * S$ where: X is an ordinal numbering of the samples and equals 0 to N-1; and $S = 2^R$ where R is M/N; and

b) replacing $A'[X]$ by $A''[X] = A'[X] + V/S^X$ for $X > 0$, and

by $A''[0] = A'[0] + \text{mod } S$ for $X = 0$,

where for each of X= N-1 to 0, V is replaced by $V-V/S^X$, V initially being the value of the M bits when X=N-1.

53. A method according to any preceding claim comprising the step of recording the said combined signal on a recording medium.

54. A method according to any one of claims 1 to 52, comprising providing the said combined signal to a signal distribution system.

55. A method according to any one of claims 1 to 51, comprising providing the said combined signal to a transmission system.

56. A computer program which when run on a suitable data processor causes the processor to implement the method of any one of the preceding claims.

57. A storage medium storing a program according to claim 56.

58. Apparatus arranged to carry out the method of any one of claims 1 to 55.

59. Apparatus for processing a digital signal comprising:

an input for receiving a digital audio signal representing complete and unimpaired audio information;

a compressor and encryptor arranged to compress and encrypt the said digital audio signal arranged to produce a compressed and encrypted first audio signal, the audio information of which is substantially unimpaired compared to that of the said digital audio signal;

an input for receiving an unencrypted second audio signal; and

a signal combiner arranged to combine the said first and second audio signals to produce a combined signal comprising the said compressed and encrypted audio signal and the unencrypted second signal.

60. Apparatus according to claim 59, comprising a first signal producer operable to produce the said digital audio signal representing unimpaired audio information.

61. Apparatus according to claim 59 or 60, comprising a second signal producer operable to produce the said unencrypted second audio signal.

62. Apparatus according to claim 61, wherein the second signal producer comprises a signal impairer for impairing the said digital audio signal to produce the said second signal.

63. Apparatus according to claim 62, wherein the second signal producer comprises a further combiner for combining the said digital audio signal with a further signal which degrades the said digital audio signal to produce the said second signal.

64. A method according to claim 63, comprising a modulator for modulating the said further signal and wherein the further combiner is arranged to combine the modulated further signal with the said digital audio signal to produce the said second signal.

65. Apparatus according to claim 64, wherein the said second signal is a sampled digital signal, each sample having most significant bits (hereinafter MSBs) and less significant bits (hereinafter LSBs) and wherein the said signal combiner is operable to combine the first signal with the said second signal by replacing the LSBs of the said second signal with bits of the first signal.

66. Apparatus according to claim 65, wherein the said signal combiner is arranged to control the ratio of the number of LSBs to MSBs according to the compression ratio achieved by the said compressor.

67. Apparatus according to claim 65 or 66, wherein the said signal combiner is operable to append at least part of the first digital signal to the said second signal.

68. Apparatus according to claim 59, 60, 61, 62, 63 or 64, wherein the said signal combiner is arranged to distribute the bits of the first signal over samples of the second signal in dependence on the ratio of the total number of encrypted bits in the encrypted first audio signal to the total number of samples of the said second signal.

69. Apparatus according to claim 68, wherein the said ratio is approximated by an integer fraction M/N where M/N is less than the said ratio, and comprising the steps of selecting groups of N samples and distributing over the N samples of each group corresponding sets of M bits.

70. Apparatus according to claim 69, wherein the said signal combiner is arranged to implement the steps of

a) scaling the value A of each of the N samples according to $A'[X] = (A[X]/S) * S$ where: X is an ordinal numbering of the samples and equals 0 to N-1; and $S = 2^R$ where R is M/N; and

b) replacing $A'[X]$ by $A''[X] = A'[X] + V/S^X$ for $X > 0$, and

by $A''[0] = A'[0] + \text{mod } S$ for $X = 0$,

where for each of X= N-1 to 0, V is replaced by $V\text{-}V/S^X$, V initially being the value of the M bits when X=N-1.

71. Apparatus according to any one of claims 59 to 70, comprising a further compressor operable to compress the said second signal, the said signal combiner being arranged to combine the said first signal with the compressed second signal.

72. Apparatus according to claim 71, wherein the compression ratio of the said further compressor is dependent on the compression ratio achieved by the said, first-mentioned, compressor.

73. Apparatus according to any one of claims 59 to 72, wherein the said compressor and encryptor is arranged to produce a losslessly compressed and encrypted first audio signal

74. A data structure comprising a combination of a compressed and subsequently encrypted first digital audio signal, the audio information of which is substantially unimpaired, and an unencrypted second digital audio signal.

75. A data structure according to claim 74, wherein the first signal is embedded in the second signal.

76. A data structure according to claim 74, in which the MSBs of the samples of the combined signal represent the second signal and the LSBs of the samples represent the first signal.

77. A data structure according to claim 76, including data indicating the boundary between the LSBs and the MSBs.

78. A data structure according to claim 76 or 77, wherein the ratio of LSBs to MSBs per sample varies.

79. A data structure according to claim 74, wherein the second signal is compressed according to a data format having auxiliary data space, and the first digital signal is in the auxiliary data space.

80. A data structure according to claim 74, 75, 76, 77, 78 or 79, wherein at least part of the first digital signal is appended to the second signal.

81. A data structure according to claim 74, wherein the data is arranged in blocks each comprising a plurality of samples, the structure including data indicating the numbers of samples in the blocks.

82. A data structure according to any one of claims 74 to 81, including data identifying at least one encryption key used to encrypt the first digital audio signal.

83. A data structure according to claim 81 or 82, wherein the blocks comprise groups of N samples and sets of M bits of the first signal are distributed over the N samples of each group where the ratio M/N is an integer fraction.

84. A data structure according to claim 83, comprising data indicating the blocks.

85. A data structure according to any one of claims 74 to 84, wherein the second signal is an impaired version of the audio signal represented by the digital signal.

86. A method of recovering a first signal from a combination of a first, compressed and encrypted, digital audio signal combined with a second signal, the audio information of the first audio signal being substantially unimpaired, the method comprising the steps of separating the first signal from the combination, decrypting the separated first signal, and decompressing the decrypted first signal to recover the substantially unimpaired audio information thereof.

87. A method according to claim 86, wherein the first signal is represented by Less Significant Bits (LSBs) of the combined signal and the second signal is represented by the Most Significant Bits (MSBs) of the combined signal and comprising the step of discarding the MSBs to separate the first signal from the second signal.

88. A method according to claim 87, wherein the first signal is appended to the second signal and comprising the step of discarding the second signal.

89. A method according to claim 86, wherein the second signal is a compressed signal compressed according to a format which has auxiliary data space in which the first signal is placed, and comprising the step of extracting the first signal from the said auxiliary data space.

90. A method according to claim 86, wherein the first and second signals are combined by the method of claim 52, wherein the recovering method comprises, for each group of N samples, the steps of setting $X = 0$, setting $V = 0$, and replacing V by $V = V + A'[X] \text{ mod} S*S^X$ for each of $X = 0$ to N-1.

91. Apparatus for recovering a digital signal, the digital signal being compressed and encrypted and combined with a second signal, the apparatus

comprising a separator for separating the compressed and encrypted signal from the second signal, a decryptor for decrypting the separated signal and a decompressor for decompressing the decrypted signal.

92. A program which when run on a suitable data processor implements the method of any one of claims 86 to 90

93. A storage medium storing a program according to claim 92.

94. Apparatus arranged to implement the method of any one of claims 86 to 90.

95. In a system comprising at least first and second processors, a method of transferring a digital signal representing content from the first processor to the second processor the method comprising the steps of:

using the first processor to implement the method of any one of claims 1 to 58 to produce the combined signal and to associate an identifier with the combined signal for identifying the combined signal;

storing the said identifier;

transferring the combined signal to the second processor;

at the said second processor, deriving the said identifier associated with the combined signal;

subject to predetermined conditions being satisfied, transferring to the second processor at least one key associated with the said identifier, for decrypting the encrypted first signal; and

using the second processor to separate the first signal from the second signal and to restore the first signal.

96. In a system comprising a transaction server and at least first and second clients, a method of transferring a digital signal representing content from the first client to the second client the method comprising the steps of:

using the first client to implement the method of any one of claims 1 to 58 to produce the combined signal and associating an identifier with the combined signal for identifying the combined signal;

providing, to the transaction server, the identifier and at least one key for decrypting the encrypted signal and storing, in the transaction server, the said identifier and the said at least one key;

transferring the combined signal to the second client;

deriving the said identifier associated with the combined signal;

transferring the identifier from the second client to the transaction server;

subject to predetermined conditions being satisfied, transferring from the transaction server to the second client at least one key associated with the said identifier, for decrypting the encrypted first signal; and

using the second client to separate the first signal from the second signal, and use the decryption key decrypt the first signal, decompress the decrypted to restore the digital signal.

97. A method of processing a digital signal comprising the steps of

providing a first digital signal representing first information,

providing a second digital signal, and

embedding the first signal in the second signal by replacing Less Significant Bits (LSBs) of the second signal by bits of the first signal and retaining the More Significant Bits (MSBs) of the second signal,

whereby the first signal occurs as noise in the second signal.

98. A method of processing a digital signal comprising the steps of

providing a first digital signal representing first information,

providing a second digital signal, and

embedding the first signal in the second signal by selecting groups of N samples and distributing over the N samples of each group corresponding sets of M samples of the first signal, where the ratio M/N is an integer fraction.

99. A method according to claim 98, comprising the steps of

a) scaling the value A of each of the N samples according to A'[X] = (A [X]/S) * S where: X is an ordinal numbering of the samples and equals 0 to N-1; and $S = 2^R$ where R is M/N; and

b) replacing A'[X] by A''[X] = A' [X] + V/S^X for X > 0, and

by A''[0] = A'[0] + mod S for X = 0,

where for each of X= N-1 to 0, V is replaced by $V-V/S^X$, V initially being the value of the M bits when X=N-1..

100. A method according to claim 97, 98 or 99 wherein the first signal is a compressed signal.

101. A method according to claim 97, 98, 99 or 100, wherein the first signal is an encrypted signal.

102. A method of processing a digital signal comprising the steps of

providing a first digital signal representing substantially unimpaired first information, the first signal being a compressed and/or encrypted signal,

providing an unencrypted second digital signal representing second information, and which is compressed according to a compression format having auxiliary data space, and

combining the first signal comprising the said substantially unimpaired first information with the second signal, embedding at least part of the first signal being embedded in the said auxiliary data space of the second signal.

103. A method according to claim 102, wherein part of the first signal is appended to the second signal.

104. A method according to any one of claims 95 to 103 wherein the first signal represents a computer program.

105. A method according to any one of claims 95 to 104 wherein the second signal is an audio signal.

106. Apparatus arranged to implement the method of one of claims 95 to 105.

107. A computer program which, when run on a suitable computer or computer system, implements the method of one of claims 95 to 105.

108. A recording medium on which the computer program of claim 107 is recorded.

109. Apparatus substantially as hereinbefore described with reference to the accompanying drawings.

110. A method substantially as hereinbefore described with reference to the accompanying drawings